Office, Assistant Secretary of the Army (ALT)
SUMMARY OF ACTION

To: ASA(ALT) Thru: MILDEP Thru: COL. DeFatta	ACTION OFFICER: MAJ. Jost OFFICE SYMBOL: SAAL-SO PHONE NO: 703-614-0154 DATE/TIME: 05 APR 02 / 1200HRS	SUSPENSE DATE CONTROL NO. 30102605

SUBJECT: DRAFT ~ Army Anti-Tamper Policy Letter

RECOMMENDATION: Review draft policy; provide concurrence or non-concurrence with specific issues.

XXXX	ACTION		INFO	DRIVE LOCATION	Global on 'Saalt2\Data_two\Share' (G:)\ARMY A-T POLICY

SUMMARY OF ACTION: Per request of Mr. Bolton, an Army Anti-Tamper Policy must be defined in order to develop guidelines and provide proper dissemination of information necessary for program offices to adequately incorporate anti-tamper techniques into their respective programs. The following draft policy letter is provided to meet this requirement. Additionally, existing policy letters are attached as background information pertinent to this requirement.
Enclosures:
Tab A – Dr. Gansler memorandum dated 04 FEB 1998 on "Implementation of Anti-Tamper (AT) Techniques in Acquisition Programs."
Tab B – Dr. Gansler memorandum dated 01 May 1999 on "Guidelines for Implementation of Anti-Tamper (AT) Techniques in Weapon Systems Acquisition Programs."
Tab C – Assistant Secretary of the AF, Lawrence DeLaney memorandum dated 27 April 2001 on "DoD Anti-Tamper (AT) Policy."
Tab D – Dr. Oscar memorandum dated 15 Oct 2001 on "DoD Anti-Tamper (AT) Policy – ACTION MEMORANDUM."
Tab E – Draft "Center of Excellence" & draft "Anti-Tamper Validation Process" PowerPoint presentations.

MILITARY DEPUTY ACTION	G-4 ACTION
[Approved] [Disapproved] [Recommend Approval] [Recommended Disapproval] PSM Noted Comments:	

COORDINATION

CC	NCC	OFFICE	NAME	PHONE
		SAAL-SO	WALLACE HANGER	703-614-0152
		SAAL-RP	YVONNE JACKSON	703-604-0158
		DCS, G2 DAMI-CHS	ROD ROBERTS	703-601-2401
		SAAL-ZR	DONALD DAMSTETTER	703-697-0387
			COL DAMIAN BIANCA	703-604-
		OGC	LEVATOR [illegible] Deputy General Counsel (Acquisition)	703-[illegible]
		HQAMC AMCOPS-FSF	JOSEPH KAECK	703-617-2020

APPROVALS

	A	D	INT. Date		A	D	INT. Date
DASA							
Asst. DASA	✓						
DASA XO	✓						

CC = Concur NCC = Nonconcurr A = Approved D = Disapproved

MS Word SAAL FORM 5

Version Dated 18 March 2002

DEPARTMENT OF THE ARMY
OFFICE OF THE ASSISTANT SECRETARY OF THE ARMY
ACQUISITION LOGISTICS AND TECHNOLOGY
103 ARMY PENTAGON
WASHINGTON, DC 20310-0103

REPLY TO ATTENTION OF

SAAL-SO

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Army Acquisition Executive (AAE) Policy Memorandum 03-X, Army Anti-Tamper (AT) Program Implementation

The purpose of the enclosed document is to establish an Army AT Policy guidance in accordance with the Department of Defense (DoD) AT Policy memorandum dated April 27, 2001. It establishes the review process for Army weapon systems and technologies to ensure that the unintentional transfer of associated technologies and/or information protected from disclosure by the Arms Export Control Act (Title 22, U.S. Code 2751) and implementing regulations does not occur.

The AT program's goal is to identify and quantify probable system critical technologies in their "expected" operating environments. This will allow the Army to make informed tradeoffs that support system design and/or modification decisions upfront and early.

The critical players in this effort are: All Project Managers, project officers or equivalent (PM's); user representatives; and the Army commands providing material development support functions. I expect aggressive leadership from the PM's to ensure that Army systems are protected from proliferation and exploitation, for as long as possible, so they can effectively perform their missions in various operational environments.

To the degree possible, and when appropriate, the costs associated with engineering AT protective measures into Army weapon systems will be borne by all users of the system, including foreign users, subject to the restrictions of the DoD Financial Management Regulation (Volume 15, Chapter 7).

Claude M. Bolton, Jr.
Assistant Secretary of the Army
(Acquisition, Logistics and Technology)

Enclosure

DISTRIBUTION:
OFFICIALS OF HEADQUARTERS, DEPARTMENT OF THE ARMY
Chief of Staff, Army
DISTRIBUTION: (CONT)
Vice Chief of Staff, Army
Assistant Secretary of the Army (Civil Works)
Assistant Secretary of the Army (Financial Management and Comptroller)
Assistant Secretary of the Army (Installations and Environment)
Assistant Secretary of the Army (Manpower & Reserve Affairs)
Office of General Counsel
Administrative Assistant to the Secretary of the Army
Office of the Chief Information Officer/G-6 (CIO/G-6)
The Inspector General
The Auditor General
Deputy Under Secretary of the Army (Operations Research)
Chief of Legislative Liaison
Chief of Public Affairs
Director, Small and Disadvantaged Business Utilization
Director of Army Staff
Deputy Chief of Staff, G-1
Deputy Chief of Staff, G-3
Deputy Chief of Staff, G-4
Deputy Chief of Staff, G-8
Deputy Chief of Staff for Intelligence
Assistant Chief of Staff for Installations Management
Chief of Engineers
The Surgeon General
Chief, National Guard Bureau
Chief, Army Reserve
The Judge Advocate General
Chief of Chaplains

COMMANDER,
U.S. Army Materiel Command, ATTN: AMCCG, 5001 Eisenhower Avenue, Alexandria, VA 22333-0001
U.S Army Forces Command, ATTN: AFCG, Fort McPherson, GA 30330-1062
U.S. Army Medical Command, 2050 Worth Road, Fort Sam Houston, TX 78234-5069
U.S. Army Intelligence & Security Command, ATTN: IACG, 8825 Beulah Street, Fort Belvoir, VA 22060-5246
U.S. Army Investigation Command, 6010 6th Street, Fort Belvoir, VA 22060-5058
U.S. Army Military District of Washington, Fort Lesley J. McNair, Washington D.C. 20319-5056
U.S. Military Traffic Management Command, ATTN: MTCG, Hoffman Building II, 200 Stovall Street, Alexandria, VA 22332-5000
U.S. Army Space and Missile Defense Command, P.O. Box 15280, Arlington, VA 22215-0280
U.S. Army Training and Doctrine Command, ATTN: ATCG, Fort Monroe, VA 23651-5000
Eighth United States Army, Unit 15236, APO AP 96205-0009

DISTRIBUTION: (CONT)
U.S. Army Pacific, ATTN: APCG, Fort Shafter, HI 96858-5100
U.S. Army South, ATTN: SOCG, Fort Buchanan, PR 00934
U.S. Army Corps of Engineers, ATTN: CECG, 441G Street, NW, Washington, D.C. 20314-1000
U.S. Army Special Operations Command, ATTN: AOCG, Fort Bragg, NC 28310

PROGRAM EXECUTIVE OFFICER,
Air and Missile Defense, ATTN: SFAE-AMD, P.O. Box 1500, Huntsville, AL 35807-3801
Ammunition, ATTN: SFAE-AMO-P, Picatinny Arsenal, NJ 07806-5000
Aviation, ATTN: SFAE-AV, Redstone Arsenal, AL 35898
Chemical and Biological Defense, ATTN: CBD, Falls Church, VA 22041-3202
Combat Support and Combat Service Support, ATTN: SFAE-CSS, Warren, MI 48397-5000
Command, Control and Communications Systems, ATTN: SFAE-C3T, Fort Monmouth, NJ 07703-5401
Enterprise Information Systems, ATTN: SFAE-PS, Fort Belvoir, VA 22060-5526
Ground Combat Systems, ATTN: SFAE-GCS, Warren, MI 48397-5000
Intelligence, Electronic Warfare and Sensors, ATTN: SFAE-IEW&S, Fort Monmouth, NJ 07703-5301
Soldier, ATTN: SFAE-P, Fort Belvoir, VA 22060-5852
Tactical Missiles, ATTN: SFAE-MSL, Redstone Arsenal, AL 35898-8000

CF:
HQDA, SAAL-ZAC
HQDA, SAAL-ZL
HQDA, SAAL-ZM
HQDA, SAAL-ZN
HQDA, SAAL-ZS
HQDA, SAAL-ZR
HQDA, SAAL-ZT

6 January 2003

SUBJECT: Initial Guidance for the Anti-Tamper (AT) Program Initiative

1. PURPOSE.

1.1 This initial guidance establishes the policy for implementation of the Army Anti-Tamper (AT) Program and the review procedures associated with the program. This policy supersedes the 07 May 1999 policy letter. It will remain in effect until 01 October 2004, at which time all Army systems will have addressed AT concerns in accordance with this guidance, and appropriate publications will contain necessary instructions to ensure future compliance. AT will be included in next generation policy and information documents.

1.2 This policy guidance provides for the AT protection of selected sensitive technologies in U.S. weapons systems that may be developed with or sold to foreign governments or that may fall into enemy hands. These guidelines apply to system performance, materials, hardware, software, algorithms, design and production methods, maintenance and logistical support, and other facets as determined by the appropriate acquisition authority.

2. OBJECTIVE.

The goal of the AT program is to ensure that Army materiel/systems will accomplish intended operational missions in peace and war without relinquishing critical technological information essential to maintaining an over-match capability against any adversary. This will be achieved by:

2.1 Defining anti-tamper requirements, techniques and procedures for all Army materiel/systems during research and development, integration, operations, training, transport, and storage.

2.2 Identifying expected system technological advances and degradation of use; taking action to protect the critical technologies (APPENDIX E/F) during these various stages of development.

2.3 Incorporating AT monitoring, controls and penalties into the acquisition and life cycle processes. The procurement approval authority for sub-systems and component parts.

Note: The procurement approval authority for sub-systems and component parts of larger systems and support equipment shall ensure that coordination is made with the PM's (project /product manager, project officer, items manager or equivalent).

3. SCOPE.

3.1 This policy shall apply to all program categories of DoD acquisition programs using critical technologies whether the program is in development or undergoing P3I or other technology insertion. The Policy will initially focus on tactical and strategic weapon systems.

3.2 Revisions to the Policy will be applicable to Command, Control,

Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) and Automated Information Systems (AIS) acquisition programs; Program Managers of C4ISR and AIS acquisition programs are encouraged to assess their programs for inclusion of AT before being specifically required to do so.

3.3 Tailoring of the acquisition strategy to more efficiently meet the AT program requirements is encouraged. AT program requirements shall be considered at all system milestone reviews and shall apply for all material procurements.

4. DEFINITIONS.

Terms used in this Policy are defined at APPENDIX A.

5. PHILOSOPHY.

5.1 The Department of Defense (DoD) actively seeks to include foreign allies and friends as partners in the development, acquisition, and life-cycle management of weapon systems. Early involvement with foreign partners is encouraged by DoD, and such cooperative partnership should begin at the requirements definition phase whenever possible. Such involvement results in benefit from shared development costs, reduced production and procurement costs realized from economies of scale, and strengthened domestic industrial bases.

5.2 AT techniques are most cost effective if developed with the system and become much more difficult/expensive if retrofit of a fielded system is required. Critical technology susceptibilities must be addressed to reduce the possibility of tampering that would put U.S. technological advantages at risk. Critical technology susceptibilities can be reduced through a variety of techniques, procedures (both manufacturing and operational) or a combination of the two. The probability of critical technology protection and mission success depends on a number of factors including AT. All these factors should be weighed to determine the degree of AT protection necessary to ensure continued U.S. technological advantage.

5.3 It is neither practical nor feasible to make every system/subsystem impervious to tampering efforts. PM's, in coordination with the user representatives and the Army command performing the materiel development role, must conscientiously assess the critical technology exploitation risk to their system, must build in protection against the risk, or must document the risk as being acceptable. The most stringent intended use of the system/subsystem will be used to identify shortcomings with respect to AT. PM'S must take actions to assure that their items are developed and maintainable at an acceptable level of AT throughout the system's life cycle.

5.4 An anti-tamper validation process and council is being established by OSD to provide program managers' access to information to assist in formulating a viable AT plan. The Army will be an integral part of this process and the council in order to conduct effective AT validation in support of Army program protection plans (APPENDIX D).

6. POLICY.

6.1 An Army Anti-Tamper Validation and Verification (AT V&V) Team shall be

formed in order to develop the AT validation and verification process for the Army. The AT V&V Team will consist of a Lead Technical Agent and various field experts from a variety of technologies. The AT V&V Team will coordinate directly with the OSD V&V Council (APPENDIX G). The core group of experts for the Army will be permanently located at Redstone Arsenal, AL, with access to various other technology experts from other geographic locations on an “as needed” basis.

6.2 The Army will additionally form its own Anti-Tamper Validation and Verification (AT V&V) Board consisting of members from the AT V&V Team (chairperson), the ASA(ALT) staff, Program Manager (PM) representative, user representative, DCS G-2 representative (DAMI-CD), and other necessary advisory members. The Board will identify critical technologies and anticipated AT requirements, evaluate the feasibility of meeting the requirements, conduct cost and schedule trade-off analysis, and document recommendations to the Program Manager.

6.3 The PM shall establish AT requirements acceptable to the AT V&V Team as early in the acquisition cycle as possible, usually not later than the Milestone B decision. The PM and user representative shall include these AT requirements in applicable acquisition documents, in coordination with appropriate agencies.

6.4 PM’s will use the AT V&V Team to assess and document, by use of analysis and/or test, that their system meets its AT requirements and the potential effects of AT on mission accomplishment. Material changes, changes in mission, or changes in the threat will require re-evaluation of the system’s AT requirements. The re-evaluation must only be extensive enough to answer concerns of the AT V&V Team. The impact of the change on mission accomplishment must be evaluated and a determination made of the acceptability of any system limitations caused by the change.

6.5 PM’s shall establish a process to maintain AT protection throughout the system using documentation, training, configuration controls and verification. The AT protection of each Army system shall be maintained throughout its life cycle as an integral activity of normal maintenance. The AT requirements shall be developed and incorporated as identifiable sections/chapters of the classified Program Protection Plan (PPP) for the Maintenance Plan and/or the Integrated Logistic Support Plan (ILSP) of each Army system.

6.6 AT related incidents (or “presumed” AT related incidents) shall be reported by maintenance personnel and/or operators at all levels through established command or management reporting systems. Respondents must be directed by the PM /user representative/materiel developer to reference the deficiency as an AT problem to allow prompt identification and investigation by AT point of contacts (POCs). Copies of reports on incidents shall be provided to DASA/DE&C (SAAL-NP).

6.7 The Army AT Manager (SAAL-SO) shall assist the Army Staff, MACOMs and other Army organizations by advice of trends with various AT techniques and procedures as a result of its coordination at Joint, national and international levels; and with awareness of the susceptibility levels identified by the AT program, ensure that the AT management process disseminates appropriate alerts and coordination.

7 IMPLEMENTATION.

7.1 AT is a systems engineering activity that must be initiated at the earliest

possible opportunity in a program's requirements definition phase. AT is applicable to Pre-Planned Product Improvement (P3I) upgrades or other technology insertion to fielded programs. PM, with support from the AT V&V Team, will determine if AT is applicable to their system and develop a plan to ensure that the system adequately protects the critical technology for that system. Some systems, primarily those with no critical technologies, will not require AT implementation. AT involves risk analysis, and the decision not to implement AT must be based on risks involved as well as on other factors including, but not limited to, feasibility, cost, performance impacts on the system, and schedule impacts. The PEOs or designated commanders are responsible for oversight of systems under their control and therefore are responsible for the decision of whether to implement AT measures or not. ASA(ALT) is responsible for oversight of the Army AT Program and will assess AT programs during milestone reviews as the Milestone Decision Authority (MDA).

7.2 Systems in Acquisition. All systems in acquisition with a Milestone B or equivalent shall fully comply with the provisions of this policy for that milestone review. This will include defining the expected critical technologies, designing the system to operate acceptably with necessary AT measures, scheduling system testing based upon the AT approach, and establishing a life cycle control process to ensure that the system will continue to operate with the appropriate AT implementation. AT whether implemented or not, will be a discussion item at milestone B and C decision points (FIGURE 2). If required:

7.2.1 At Milestone B, AT shall be addressed in conceptual terms of how it is to be implemented; working prototypes appropriate to this stage of program development should be demonstrated.

7.2.1.1 AT final requirements should be fully disclosed at the decision review prior to the MS B decision.

7.2.2 At Milestone C, AT implementation shall be fully documented, tested, and ready for production; the Milestone C decision shall not be given favorable consideration until AT implementation is successfully and satisfactorily demonstrated.

7.2.2.1 The AT implementation plan should be fully disclosed at the Critical Design Review prior to the MS C decision.

7.3 Fielded Systems. Development systems already fielded with a Milestone B or equivalent will not be required to implement AT because AT may be difficult or impossible to retrofit. However, AT shall be considered in any product improvement engineering effort for these systems. The use of AT may be required for programs, regardless of their acquisition status, at the discretion of the MDA.

7.4 AT shall be considered for use on any system developed with allied partners, likely to be sold or provided to U.S. allies and friends, or to fall into enemy hands. If the system is not likely to be exposed to these scenarios, then AT may not be required. This decision, however, must be deliberate, fully supported, and documented in the AT classified annex to the PPP. The classified annex will not be releasable to foreign nationals, and will include guidance for use by PM's on AT information that cannot be discussed with allies.

7.5 U.S. weapons systems in acquisition with a Milestone B or equivalent not intended for foreign distribution through FMS, DCS, or other avenues, but may fall into enemy hands on the battlefield shall include AT if critical technologies are involved.

8 RESPONSIBILITIES.

8.1 Assistant Secretary of the Army (Acquisition, Logistics, Technology) ASA(ALT): act as proponent for the Army AT Program for policy and standards; provide the Executive Secretary (SAAL-SO) for the AT V&V Team, chaired by the Lead Technical Agent; oversee implementation of AT policy and institutionalization of the Army AT Program; and ensure that revisions of AR 70-1, Systems Acquisition Policy and Procedures, and other publications contain appropriate provisions for the Army AT program; notify SAAL-NP of AT guidance that must be incorporated into export policy documents for Army weapon systems.

8.2 Commanding General, U.S. Army Material Command (HQ AMC): maintain AT Oversight Management Office, which will serve as technical proponent for AT program, policy and standards and as AT program advisor to ASA(ALT); develop and maintain scientific/engineering personnel, analysis, and test facility resources to accomplish the implementation of AT policy; ensure coordination is made with PM's before repair parts, support equipment and other government furnished items are procure.

8.2.1 U.S. Army Material systems analysis Activity: support AT policy and provide the technical independent evaluator for material acquisition programs as required.

8.2.2 U.S. Army Test and Evaluation Command: support AT policy and provide the technical tester for material acquisitions programs as required.

8.2.3 U.S. Army Logistics Management College (ALMC): support AT policy and provide technical training for personnel involved in the research, development, acquisition, and management of Army systems as required.

8.2.4 Other Major Subordinate commands: support AT policy and provide scientific/engineering technical support for material acquisition programs as required by HQ AMC, AT V&V Team.

8.3 Commanding General, U.S. Army Training and Doctrine Command (TRADOC): ensure the inclusion of AT concerns in the requirement documents for each Army system; provide members to various AT V&V boards that will determine AT requirements for systems and conduct trade-offs as necessary, ensuring that the systems can perform assigned missions while maintaining the appropriate level of AT; and development of curriculum in TRADOC schools for AT awareness training and training of personnel on the installation, operation and maintenance of Army systems. Foreign nationals will not be allowed to participate in TRADOC courses. (Exceptions to this rule may be requested from the ASA(ALT), but will be considered from a presumption of denial).

8.4 Office of the Chief Information Officer/G-6 (CIO/G-6): provide the information systems management focal point for the implementation of this policy for assigned systems.

8.5 Commanding General, U.S. Army Information Systems Command (INSCOM): responsible for the implementation of this policy for assigned systems.

8.6 Commanding General, U.S. Army Operational Test and Evaluation Command (ATEC): as operational evaluator is responsible for ensuring that material meets the

requirements established in this policy for effective AT protective measures through the continuous and comprehensive evaluation of the acquisition process and through operational test and evaluation, prior to full scale production and fielding.

8.7 Commander, U.S. Army Safety Center: monitor the application of system safety throughout the life cycle including the effects of AT implementation; and provide HQDA level guidance for addressing/evaluating AT concerns and ensuring risk assessment procedures are in accordance with AR 385-16.

8.8 Program Executive Officer/PM: execute and manage the application of policies contained in this initial guidance to achieve the stated objectives for each Army system, regardless of where it may be in its life cycle (APPENDIX C).

8.9 Army Special Program Office (SAAL-SO), Director: Executive Secretary (SAAL-SO) for the AT V&V Team; oversee implementation of AT policy and institutionalization of the Army AT Program on behalf of the AAE; provide information on AT measures for specific weapons systems to SAAL-NP.

8.10 AT V&V Team: meet as necessary to determine AT criteria, determine the impact of material, environmental or mission changes on the criteria, conduct trade-off analysis, and provide written recommendations to the PM/PEO.

9 REQUIREMENTS.

9.1 The AT V&V Board for each system is composed of the members from the AT V&V Team (chair person), ASA(ALT) staff, PM, user representative, DCS G-2 representative (DAMI-CD), and other necessary advisory members. The Board will identify critical technologies and anticipated AT requirements, evaluate the feasibility of meeting the requirements, conduct cost and schedule trade-off analysis, and document recommendations to the PM. Any decision not to fully comply with the AT requirements will be treated as an inadequacy of the system. Relaxation of AT requirements will be considered for approval only when there is an overriding benefit to the government.

9.2 The decision to use or not to use AT will be documented in a classified annex to the PPP (Appendix D). The PM should use the AT V&V Team to conduct the technology assessment and advise whether or not the implementation of AT is required.

9.3 AT applicability will be assessed for each modification or P3I upgrade to the production system. It is feasible that AT may be discontinued when it is assessed that the technology no longer needs to be protected. The PM should use the AT V&V Team to conduct the technology re-assessment and advise whether or not to continue implementation of AT requirements.

9.4 AT Requirements. AT requirements are drawn from the approved projections of the AT V&V Team. The AT requirements are based on the predicted environment for the intended development, operation, training, transport, and storage phases of the system, expected throughout the system life cycle.

9.4.1 The recommendation to implement or not to implement will be validated by the MDA. SAAL-SO will keep abreast of AT as part of its oversight role on behalf of the AAE.

9.4.2 ASA(ALT) and the director of SAAL-SO shall be kept apprised of the status of AT in all programs, including AT implementation in a SAP. Personnel in these offices shall be granted access to the SAP in order to perform oversight functions should AT be implemented or should the AT technology itself require a SAP.

9.5 Relaxation of AT Requirements.

9.5.1 Justifications. Only the AT V&V Team may determine that a relaxation of AT requirements is appropriate. Relaxation approval authority for AT remains with the designated Milestone Decision Authority (MDA). Relaxation of AT requirements will not be approved if the deficiency would result in the potential compromise of a critical technology being compromised to foreign entities. If a relaxation of AT requirements conflicts with a material requirement, a request for change to the requirement must also be approved in accordance with AR 71-9. Relaxation of the AT requirements may be justified under the following conditions:

9.5.1.1 Operational justification. Deployment, use, temporary disconnection, or other means to operationally reduce the tamper threat, in lieu of protecting to higher levels. If a system will not be available for a period of time, an assessment of mission impact will be made for the duration of periods of expected non-availability. The PM and user representative must ensure that systems are identified as AT restricted items and that equipment operators and commanders are made aware of the potential limitations.

9.5.1.2 Proliferation Justification. If a capability/technology is deemed “available on the open market” or no longer consider “leading edge technology” by the AT V&V Team, consideration for relaxation of AT requirements for that system can be recommended to the MDA by the PM.

9.5.2 Process. The AT V&V Team will evaluate the impact of any proposed relaxation on the basis of mission accomplishment and technology protection. The Team will make a written recommendation to the PM on whether a relaxation should be pursued. The following steps will be taken in conjunction with Army request to relax AT requirements by the PM:

9.5.2.1 Army command performing materiel development roles: Provide technical support for PM’s of systems; provide a technical representative for the AT V&V Team for those systems.

9.5.2.2 PEO: Resolve any concerns raised by the AT V&V Board; and ensure that the PM’s justification includes evaluation results.

9.5.2.3 AT V&V Team: Convenes to define system AT requirements in conjunction with AT V&V Board and acts as chairperson for the Board. The Team will:

9.5.2.3.1 Perform and/or review technical analyses;

9.5.2.3.2 Verifies the scope and effectiveness of the system AT effort;

9.5.2.3.3 Validate requests for relaxation of AT requirements justification(s) for all systems;

9.5.2.3.4 Provide written recommendations and comments to the responsible PM;

9.5.2.3.5 Forward written recommendations and comments to the responsible Program Executive Officer/Commander having program authority for the system if the concerns of all the members are not resolved by the PM;

9.5.2.4 Submit unresolved concerns for ACAT I and ACAT II programs and concerns to ASA(ALT) if the concerns are not resolved at the PEO/ Commander level.

10 TEST AND EVALUATION.

10.1 To ensure that the Army material is in compliance with AT policy, analysis and testing under the purview of an Army tester and the AT V&V Team shall be performed on samples of each Army system that is required to implement AT based upon the performance statement of the material requirement. Analyses will assess the probable inter-system and intra-system AT requirements, as well as provide guidance and theoretical pretest predictions. The intent of AT testing is to use currently scheduled testing to ensure that AT is fully addressed against the AT requirements rather than requiring new or increased testing. Testing may be divided into two categories:

10.2 Developmental Test and Evaluation: There are two distinct types of developmental tests:

10.2.1 Developmental tests and analyses, are the responsibility of the PM, are performed at Government laboratories, Government test centers, or equivalent contractor operated facilities. These cooperative tests validate analyses, identify AT that are not amenable to analysis (for example, most non-linear effects), and develop AT levels.

10.2.2 Developmental tests and evaluation, are conducted in the developmental environment by technical personnel under the purview of an Army tester and the AT V&V Team. These tests are performed against AT requirements and standards developed for the system and may be contractually binding. Facilities performing this class of test must avoid the fact or appearance of conflict of interest.

10.3 Operational Test and Evaluation: tests conducted in an operational environment by operational Army units under the purview of an Army Operational Tester and the AT V&V Team.

11 TRAINING.

AT awareness training, is available upon request to either the AT V&V Team or SAAL-SO. AT V&V Team members are available to deliver presentations on critical technology identification, re-engineering techniques, risk assessment and AT adaptation to systems.

12 SYSTEM ENGINEERING MANAGEMENT.

12.1 The PM shall be responsible for managing the total engineering effort during the life cycle. The PM shall ensure that system engineering as applied to AT is adequately planned, executed, and verified so as to result in AT protection that meets operational and supports needs. AT requirements validation and risk assessment will be managed as key elements of the system engineering management effort, integral to the overall system acquisition.

12.2 Figure 1 is a representative “generic decision process” for determining whether or not to implement AT in a program. Management of the AT decision and implementation processes shall be at the discretion of the MDA.

12.2.1 To fully support the systems engineering approach used to define the AT concept, participation of the AT V&V Team and the program’s Overarching Integrated Process Team (OIPT) is highly encouraged.

13 MAINTAINING OPERATIONAL SYSTEMS.

13.1 Appropriate actions must be taken by PM’s, user representatives, material developers, and item managers to reduce to an acceptable level the risk associated with technology proliferation throughout the operational life of the equipment. These managers must assure that their items are maintainable in design and are maintained in practice at an acceptable level of readiness to operate in the anticipated AT environment throughout the life cycle.

13.2 It may be necessary to limit the level and extent of maintenance a foreign customer performs in order to protect critical technologies. This may mean that the level of maintenance that involves the AT protected assembly or component will only be accomplished by the U.S. contractor or U.S. government facility in the United States or overseas.

13.2.1 Maintenance and logistics restrictions must be stated in the appropriate contracts (PA, MOA, MOU, export license, or other similar document).

13.2.2 The restrictions stated in 13.2.1 will protect the U.S. Government and U.S. industry against warranty and performance claims in the event AT measures are activated by unauthorized maintenance or other intrusion. Such unauthorized activities may be regarded as attempts to exploit the weapons system or the AT technique itself and shall void warranties and performance guarantees.

13.3 AT related incidents (or “presumed” AT related incidents) shall be reported by maintenance personnel and/or operators at all levels through established command or management reporting systems. Respondents must be directed by the PM/user representative/materiel developer to reference the deficiency as an AT problem to allow prompt identification and investigation by AT point of contacts (POCs).

13.3.1 End-Use Monitoring (EUM) programs of the USG shall be used to the maximum extent possible to identify AT related incidents. These EUM programs include the Blue Lantern program (managed by the Department of State to verify end-use for defense

hardware exported commercially), and the Golden Sentry program (managed by the Department of Defense to verify end-use for articles provided via FMS channels).

14 GUIDELINES FOR AT DISCLOSURE:

14.1 The fact that AT has been implemented in a weapons program developed with allied partners shall be unclassified, subject to the discretion of the program's MDA. The techniques and methods used to implement AT, however, may be classified up to and including a Special Access Program (SAP) as appropriate, and will not be disclosed to any non-U.S. entity without specific prior approval from the program's MDA in coordination with ASA(ALT). Disclosure of information regarding protective AT measures for specific weapon systems must not be discussed with a prospective customer before an LOA or direct commercial sale is finalized.

14.2 Weapons systems developed without foreign participation, but sold overseas through the Foreign Military sales (FMS) or Direct Commercial Sales (DCS) process, will follow the same guidelines specified in paragraph 14.1 for AT acknowledgement and non-disclosure of techniques and methods.

14.3 In some cases a separate bilateral security agreement between the U.S. and a foreign ally may be required to address AT protection of a specific weapons system sold through FMS channels.

15 HQDA (SAAL-SR) point of contact for Army Anti-Tamper initiatives is Mr. Ron Mlinarchik, (703) 604-8118.

APPENDIX A: EXPLANATION OF ABBREVIATIONS AND TERMS

Anti-Tamper Techniques: Systems engineering activities intended to prevent and/or delay exploitation of critical technologies in U.S. weapons systems.
AIS: Automated Information Systems
ASA(ALT): Assistant Secretary of the Army (Acquisition, Logistics, & Technology)
AT: Anti-Tamper techniques
C4ISR: Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance
DCS: Direct Commercial Sales
DoD: Department of Defense
FMS: Foreign Military Sales
ILSP: Integrated Logistic Support Plan
MACOM: Major Command
MDA: Milestone Decision Authority
MOA: Memorandum of Agreement
MOU: Memorandum of Understanding
OIPT: Overarching Integrated Product Team
ASA(ALT): Assistant Secretary of the Army for Acquisition, Logistics, and Technology
P3I: Pre-Planned Product Improvement
PEO: Program Executive Officer
PM: Program Manager
POC: Point of Contact
PPP: Program Protection Plan
SAAL-SO: Army Special Programs Office
SAP: Special Access Program
V&V: Verification & Validation

APPENDIX B: REFERENCES

- USD(AT&L) memorandum, “Implementation of Anti-Tamper (AT) Techniques in Acquisition Programs” (U)
- DoD 5200.1-M, “Acquisition systems Program Protection Plan” (U)
- Military Critical Technologies List, www.dtic.mil/mctl (U)
- DoD “guidelines for Implementation of anti-Tamper Techniques in Weapon systems Acquisition Programs” (U)
- AR 71-9, “Materiel Requirements” (U)

APPENDIX C: PROGRAM MANAGER'S AT RESOURCES

Laboratories. U.S. Government Laboratories conduct activities that perform one or more of the following functions: science and technology; engineering development; systems engineering; or engineering support of deployed materials and their modernization. These include laboratories; research institutes; and research, development, engineering, and technical activities. The following is a partial list of Department of Defense and Department of Energy laboratories and their locations that may potentially be of assistance to present and future weapon systems and other types of acquisition programs for Program Managers:

Office of the Secretary of Defense

1) Armed Forces Radiological Research Institute; Behtesda, MD
2) National Security Agency; Ft. Meade, MD
3) Defense Technical Information Center Militarily Critical Technologies List (www.dtic.mil/mctl)
4) Defense Technology Analysis Office; Linthicum, MD

United States Army

1) Army Research Lab (ARL); Adelphi, MD
2) ARL; Aberdeen Proving Grounds, MD
3) ARL; White Sands Missile Range, NM
4) ARL, NASA; Langley, VA
5) ARL, NASA; Lewis, OH
6) Natick Research, Development, and Engineering Center, Natick, MA
7) Aviation Research, Development, and Engineering Center; St.Louis, MO
8) Aviation Troop Command, Aeroflight Dynamics Directorate; Moffett Field, CA
9) Aviation Troop Command, Aviation Applied Technology directory; Ft. Eustis, VA
10) Edgewood Research, Development, and Engineering Center; Aberdeen Proving Ground, MD
11) Communications Electronics Command Research, Development, and Engineering Center; Ft. Monmouth, NJ
12) Communications Electronics Command Research, Development, and Engineering Center – Night Vision Electronics Sensors Directorate, Ft. Belvoir, VA
13) Missile Research, Development, and Engineering Center; Redstone Arsenal, AL
14) Armaments Research, Development, and Engineering Center; Picatinny Arsenal, NJ
15) Armaments Research, Development, and Engineering Center, Benet labs; Watervliet Arsenal, NY
16) Tank & Automotive Command Research, Development, and Engineering Center; Warren, MI
17) USA Research Institute of Infectious Diseases; Ft. Detrick, MD
18) Walter Reed Army Institute of Research; Washington D.C.
19) Institute of Surgical Research; Ft. Sam Houston, TX
20) Aeromedical Research Lab; Ft. Rucker, AL
21) Medical Research Institute of Chemical Defense; Aberdeen Proving Ground, MD
22) Research Institute of Environmental Medicine, Natick, MA
23) Construction Engineering Research Laboratory; Champaign, IL
24) Cold Weather Research and Engineering Lab; Hanover, NH
25) Topographic Engineering Center; Alexandria, VA
26) Waterways Experiment Station; Vicksburg, MS
27) Research Institute for Behavioral and Social Sciences; Alexandria, VA

28) Simulation, Training, and Instrumentation command; Orlando, FL
29) High energy Laser Systems Test Facility; White Sands Missile Range, NM

United States Navy

1) Naval Air Warfare Center, Weapons Division; china Lake, CA
2) Naval Air Warfare Center, Weapons Division; Point Mugu, CA
3) Naval Air Warfare Center, Aircraft Division; Patuxant River, MD
4) Naval Air Warfare Center, Aircraft Division; Lakehurst, NJ
5) Naval Research Lab; Washington DC
6) Naval Research Lab Detachment; Bay St. Louis, MS
7) Naval Surface Warfare Center, Carderock Division; Bethesda, Md
8) Naval Surface Warfare Center, Crane Division; Crane, IN
9) Naval Surface Warfare Center, Dahlgren Division; Dahlgren, VA
10) Naval Surface Warfare Center, Dahlgren Detachment; Panama City, FL
11) Naval Surface Warfare Center, Indian Head Division; Indian Head, MD
12) Naval Surface Warfare Center, Port Hueneme division; Port Hueneme, CA
13) Naval Surface Warfare Center; Bayview, ID
14) Naval Command, control, and Ocean Surveillance Center; San Diego, CA
15) Naval Command, control, and Ocean Surveillance Center, In-Service Engineering Division; Charleston, SC
16) Naval Command, control, and Ocean Surveillance Center, In-Service engineering division; Pearl Harbor, HI
17) Naval Aerospace Medical Research Center; Pensacola, FL
18) Naval Dental Research Lab; Great Lakes, IL
19) Naval Health Research Center; San Diego, CA
20) Naval Undersea Warfare Center, Keyport division; Keyport, WA
21) Naval Surface Warfare Center, Carderock Division, Philadelphia Detachment; Philadelphia, Pa
22) Naval Undersea Warfare Center; Newport, RI
23) Naval Research Lab, Monterey Detachment; Monterey, CA
24) Naval Air systems command (engineering functions)
25) Naval Sea systems command (engineering division)
26) Naval air warfare center Training systems division; Orlando, FL
27) Naval and clothing Textile Researc Facility; Natick, MA
28) Naval Facilities Engineering Service Center; Port Hueneme, CA
29) Naval submarine Medical Research Lab; Groton, CT
30) AEGIS; Wallops Island, WA
31) AEGIS; Morristown, NJ
32) Naval Warfare Assessment Division; corona, CA
33) Explosive Ordnance disposal Technical Center; Indian Head, MD
34) Naval Ordnance Center; Indian Head, MD
35) Naval Sea Logistics Center; Mechanicsburg, PA
36) Fleet Technical Support Center; Mayport, FL
37) Fleet Technical Support Center; San Diego, CA
38) Fleet Technical Support Center; Pearl Harbor, HI

United States Air Force

1) Air Force Research Laboratory; Wright-Patterson AFB, OH

Operating Locations:

a) Wright-Patterson AFB, OH
b) Brooks AFB, TX
c) Mesa, AZ
d) Eglin AFB, FL
e) Tyndall AFB, FL
f) Kirtland AFB, NM
g) Hanscom AFB, MA
h) Edwards AFB, CA
i) Griffiss AFB, NY

2) Aeronautical Systems Center; Wright-Patterson AFB, OH (engineering functions)
3) Electronic Systems Center; Hanscom AFB, MA (engineering functions)
4) Space and Missile Center; Los Angeles AFB, CA (engineering functions)
5) Air Armament Center; Eglin AFB, FL (engineering functions)
6) Oklahoma city air Logisitics Center; tinker AFB, OK (engineering functions, minus supply, depot maintenance, and host base support)
7) Ogden air Logistics Center; hill AFB, UT (engineering functions, minus supply, depot maintenance, and host base support)
8) Warner-Robbins Air Logisitcs Center; robbins AFB, GA (engineering functions, minus supply, depot maintenance, and host base support)

Department of Energy

1) Sandia National Labs; Kirtland AFB, NM
2) Los Alamos National Lab; Los Alamos, NM
3) Lawrence Livermore National Lab; Livermore, CA

APPENDIX D: PROGRAM PROTECTION PLAN (PPP)

Discussion: DoD 5000.2-R requires Anti-Tamper measures to be documented in a classified annex to the PPP. The Air Force, Army, Navy and Missile Defense Agency weapon system programs will submit this annex to their respective Service AT point of contact as well as to their Milestone Decision Authority (MDA). If a weapon system program has a PPP, then a classified AT annex shall be developed to incorporate this information. Programs not possessing a PPP will submit an AT Plan in lieu of the classified annex to the PPP.

Below defines the information required and format for the annex to the PPP. It will have 5 sections.

SECTION 1: Introduction

Program Name and Brief Description
Responsible Service (Army, Air Force, Navy, Missile Defense Agency, Other)
Last Milestone (A, B, C)
Program AT Point of Contact (POC) and Phone Number

SECTION 2: Documenting Decision whether or not to implement AT

Document the analysis and recommendation to use or not use anti-tamper measures in this section. Refer to DoD 5000.2-R, Section 6.7.5 for further information.

SECTION 3: Document Milestone B Required Information

Information required in this section includes:

A. Identify the critical program information and technologies associated with your specific weapon system.
B. Provide a threat analysis, incorporating the most likely threat. Combat loss is one likely threat scenario where the exploiter has one weapon system, (i.e. EP-3 landing on Hainan Island). Another likely threat scenario is the deliberate exploitation where multiple copies of the weapon system are obtained by the exploiter, such as a Foreign Military Sale (FMS).
C. Identify the vulnerabilities of your critical program information as it resides in your specific weapon system.
D. Provide the preliminary AT requirement.

SECTION 4: Document Milestone C Required Information

Information required in this section includes:

A. Updates to all information provided in SECTION 3.
B. Analysis of AT methods that apply to the system, including cost/benefit assessments.
C. Explanation of AT method(s), which have been or will be implemented.
D. AT test results from Developmental Test & Operational Test.
E. AT validation plan.

APPENDIX D: PROGRAM PROTECTION PLAN (PPP) (cont)

SECTION 5: Document Post-Milestone C Required Information

Information required for in this section includes:

A. Updates to all information provided in Section 4.
B. AT validation results.

APPENDIX E: CRITICAL LO TECHNOLOGIES

The following technologies, though not all-inclusive, are critical to achieving LO capability at a system level. The Service component LO/CLO OPR will assess component performance requirements against thresholds defined by DoDI S-5230.28 to support proper level of classification.

Materials and Structures

General

- Aircraft, missile or ship LO compatible rain erosion coatings.
- Any radar absorbing material (RAM) designed for or usable in extreme environmental conditions.
- Composites combined or formed into integral radar absorbing structures.
- LO antennas, radomes and windows.

RCS-Dielectric

- Ceramic RAM and radar absorbing structure (RAS). High temperature ceramic RAM (>300F).
- Materials which use polymers loaded with carbon fibers, dielectric RAM, graded dielectric (e.g. dipped ink) honeycomb, radar absorbing metals on cloth, Jaumann and other such designs, ceramic, reticulated foam, diamond coatings, thin films, and millimeter wave aerosols.
- RAM/RAS including, but not limited to honeycomb cores/foams, and whiskers, fibers and flakes.

RCS-Magnetic

- High temperature magnetic RAM (>300F).
- Materials that use polymers loaded with carbonyl iron powder (CIP), ferrites, iron whiskers, fibers and flakes or other magnetic additives.
- RAM and RAS including, but not limited to, magnetic particles, whiskers, fibers and flakes, magnetic films, or other resistive/magnetic materials.
- Broadband (>30% bandwidth), lightweight (<2 lbs/sq ft) magnetic RAM.
- Raw, passivated (anti-rust treated) carbonyl-iron or similar microspheres.
-

Signature Control

Acoustic – Treatments that reduce the acoustic signature by using active noise cancellation, modulation of jet or diesel engines, tracks, rotor blades or other noise sources or advanced passive acoustic absorptive techniques.

Infrared

- IR signature reduction materials and techniques including, but not limited to, paints, controllable emissivity and/or reflectivity characteristics, E-O characteristics.
- IR transparent binder.
- Electrochromatics and thermochromatics, diamond coatings.

Laser – Laser signature magnetic techniques.

APPENDIX E: CRITICAL LO TECHNOLOGIES (cont)

LO Material Manufacturing Processes – Processes that use microencapsulation or microspheres, which reduce thermal, radar, or visual detection.

Multispectral

- Multi-layer camouflage systems using different techniques to reduce vehicle detectionability, which do not impair mobility or agility of the platform.
- Multispectral surface treatments/appliqués applied to weapon system platforms to improve IR/visual and/or radar reflectivity characteristics.
- Reduction of weapon platform signature or component system due to either active or passive techniques that result in shaping, cooling, or degrading the detection in any spectrum.

Optical

- Visual, including color and dynamic variations.
- Active lighting devices.

Software

- Computer codes that use classified measured data to analyze, predict, design or optimize signature reduction solutions.
- RCS/IR measurement equipment and prediction software.

Test, Measurement, Production and Inspection

- Manufacturing process and equipment specific to producing LO components.
- Manufacturing techniques, processes, equipment and codes that use classified data to analyze, predict, design or optimize signature reduction solutions.
- Computer codes or routines enabling a potential target or device to be analyzed from an observables standpoint.
- Aspects of support equipment such as configuration, design details, operating principles, performances, and quantities disclosing classified characteristics of equipment it tests or supports.
- Items for field portable repair validation of signature reduction integrity.
- Measurement and validation test cells having integrity/accuracy.

Weapon systems Integration

- Air-to-air missile systems to include AMRAAM, AIM-9, and future air-to-air missiles.
- Air-to-ground ordinance to include the joint stand-off weapon and advanced air-to-ground ordinance.
- Electronic warfare systems to include jammers, advanced IR countermeasures, seductive jamming and spoofing, synthetic aperture radar countermeasures, high power microwave, high power frequency.
- LO-treated weapons systems for ground, sea, and air.
- Surface-to-air missile systems to include Medium Extended Air Defense Systems (MEADS).
- LO integrated systems in which functionality is enhanced or enabled by combinations of the above using trade-offs and applications to create reduced system signature. This integration may occur from conception, through system design, production to the completion of life cycle operation.

APPENDIX F: CRITICAL CLO TECHNOLOGIES

The following technologies, though not all-inclusive, are critical to achieving robust CLO capability at a system level. The Service component LO/CLO OPR will assess component performance requirements against thresholds defined by DoDI S-5230.28 to support proper level of classification.

Elemental Devices: Devices for which the application is general in nature.

- Power transistors
- Digital signal processing (DSP) chips
- Ferrite components: oscillators
- Low Noise Amplifiers (LNAs)
- Monolithic Microwave Integrated Circuits (MMICs)
- A/D & D/A converters
- Millimeter wave sources (Solid state & Tube)
- Doppler filters
- Circulators

Complex Devices/Methods: Devices/methods whose application is more specific in nature.

RF Devices:

- Exciters
- Receivers
- Electronically steered antennas
- Waveform generators
- Transmit/Receive modules
- Frequency synthesizers

RF Devices:

- Focal plane arrays
- IR domes/windows

RF Processing Techniques:

- Complex radar waveforms and processing
- Space-time adaptive processing
- Adaptive digital beamforming and nulling
- ESM for LPI waveforms
- Adaptive waveforms
- ISAR/SAR
- Super resolution

IR Processing Techniques:

- Non-uniformity compensation
- Clutter discrimination algorithms
- Multi-frame image processing

General techniques:

- Sensor fusion
- Non-cooperative target recognition
- Interference suppression
- high Power microwave (HPM)

Miscellaneous:

- Applications Specific Integrated Circuits (ASICs)
- Methods designed to exploit unique LO signature characteristics

CLO subsystems: Complex collections of devices for which performance objectives include the ability to perform a CLO function. Performance is typically determined relative to some LO signature characteristic, such as RAS. Examples of CLO subsystems are:

- RF sensors
- Fuzes
- IR sensors

APPENDIX F: CRITICAL CLO TECHNOLOGIES (cont)

CLO Systems: Collections of devices and subsystems that perform a specific CLO warfighting function. Performance is typically determined relative to some CLO signatures characteristic, such as RCS. Examples of CLO systems are:

- Surveillance radar systems (e.g. SPY-1, JSTARS)
- Fire control radars (e.g. Multi-Function Radar)
- Sensor fusion systems (e.g., Cooperative Engagement Capability)
- Missiles, directed Energy (e.g., AMRAAM, AIM-9X, ESSM, STANDARD)

CLO Systems of Systems: Groups of systems tied together functionally to create an entire CLO kill chain capability (initial detection through target kill). Examples of CLO systems of systems are:

- Ship self-defense system (e.g., NATO Seasparrow)
- Integrated Air Defense System
- Air defense weapon system (e.g., PATRIOT)

APPENDIX G: OSD ANTI-TAMPER (AT) VALIDATION TEAM AND ANTI-TAMPER VALIDATION COUNCIL

Classified S-NF

FIGURE 1: "ANTI-TAMPER" ROADMAP

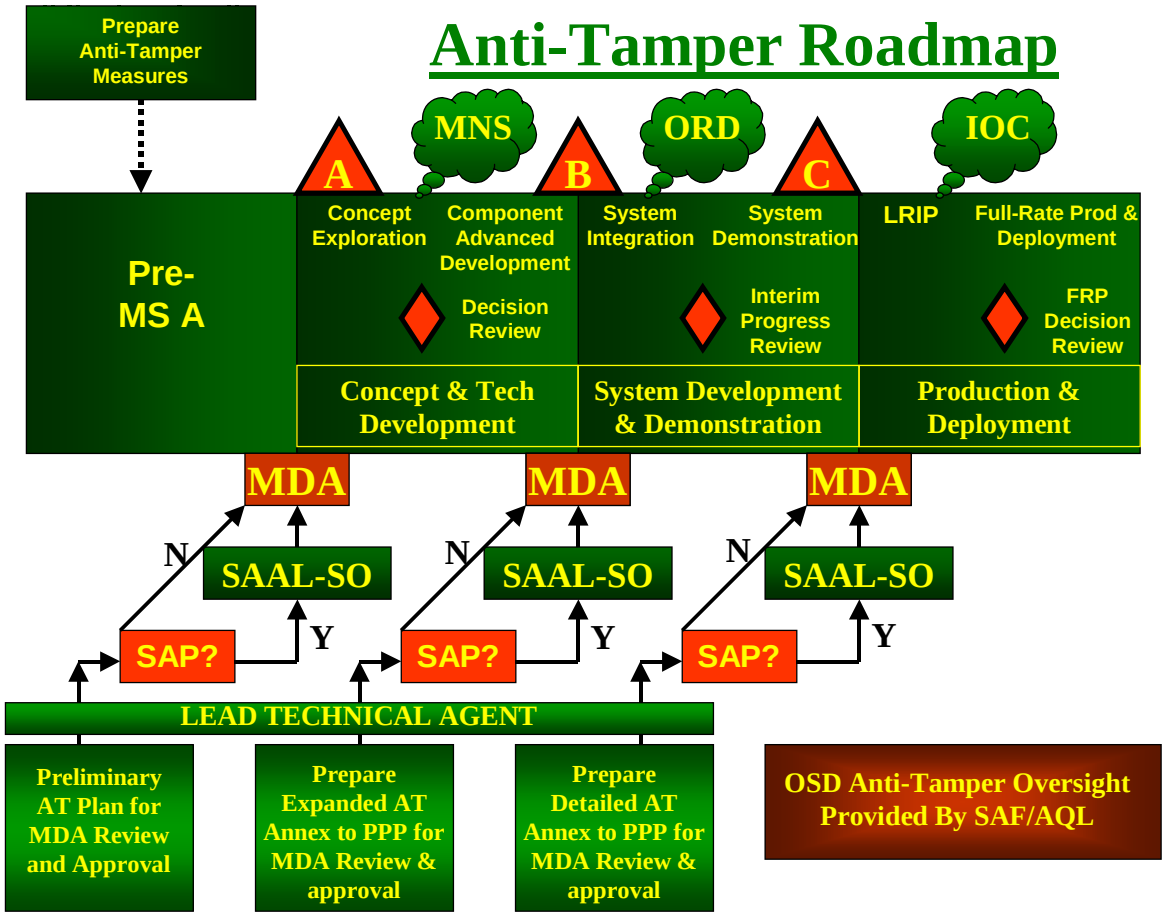

FIGURE 2: "GENERIC DECISION PROCESS"